



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,510	10/31/2001	Richard Paul Tarquini	10017331-1	7297

7590 07/14/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

ZIA, SYED

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/003,510

Applicant(s)

TARQUINI ET AL.

Examiner

Syed Zia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 25 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendment filed on April 25, 2005. Original application contained Claims 1-16. Applicant currently amended claim 10. The amendment filed have been entered and made of record.
2. Previous objection to abstract and specification and has been withdrawn.
3. Presently pending claims are 1-16.

Response to Arguments

Applicant's arguments filed on April 25, 2005 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-16 applicants argued that the system of cited prior arts [Porras (U. S. Patent 6,704,874), and Trcka et al (U. S. Patent 6,453,345)] that cited prior art appears to disclose a monitoring system having, for example, an intrusion detection system cited prior art also appears to disclose that the monitoring system that produces an alert stream that is sent via a secure electronic communication line (SSL) to an alert manager for collection, processing and distribution. Cited prior art further appears to disclose that the alert manager that is equipped with a translation module to translate original, raw data-streams received from the monitors into

Art Unit: 2131

a common format for further processing. Thus, the cited prior art system *does not appear to disclose or even suggest having an intrusion detection application for identifying a frame of data as intrusion-related' and decoding . . . the intrusion-related data"*, and cited prior art "*does not appear to perform any decoding and/or translating function to the raw data streams generated thereby*".

This is not found persuasive. The system of cited prior art does teach and describe a network based alert management method that involves consolidating alerts that indicate common incident, and generating output reflecting consolidated alerts. The alerts are received from network sensors, and the alerts that indicate a common incident are consolidated. An output reflecting the consolidated alerts is generated. The alert manager is tailored to a particular application by dynamically adding or removing data connection to sources of incoming alerts and by dynamically varying the process modules, user filter clauses, priority clauses, topology clauses and output. Therefore, the method of managing alerts in a network including receiving alerts from network sensors, consolidating the alerts that are indicative of a common incident and generating output reflecting the consolidated alerts.

The alert management system, for intrusion detection, is configurable with respect to the data needs and policies specified by the remote processing station. These processes are customizable on a per remote processing station basis. For example, two remote processing stations may in parallel subscribe to alerts from the alert management process, with each having individual filtering policies, prioritization schemes, and so forth, applied to the alert/incident reports it receives.

Art Unit: 2131

As a result, cited prior art does implement and teaches a system of signature devices and a method for generating digital signature as recited claims. Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and subsequent dependent claims. Accordingly, rejections for Claims 1-16 are respectfully maintained.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claim 10 is rejected under 35 U.S.C. 102(e) as being anticipated by Porras (U. S. Patent 6,704,874).

Art Unit: 2131

2. Regarding Claim 10 Porras teaches a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method [Fig.6, col.9 line 1 to line 20]:

identifying [sensors 22 monitoring various host/network traffic for suspicious activities] frame [streams] as an intrusion by an intrusion detection application (col.3 line 30 to line 37, and col.3 line 54 to col.4 line 1);

decoding [translation module 32] by the intrusion detection application, the intrusion-related data (col.4 line 1 to line 25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-9, and 11-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras (U. S. Patent 6,704,874), and further in view of Trcka et al (U. S. Patent 6,453,345).

Art Unit: 2131

4. Regarding Claim 1 Porras teaches a method of detecting network-intrusions [detecting suspicious activities, such as intrusion, and based on that generating digital alerts] (Fig.1 Item 22, and col.1 line 26 to line 28) at a first node of a network [Fig. 1, item 12], comprising:

identifying [sensors 22 monitoring various host/network traffic for suspicious activities] frame [streams] as an intrusion by an intrusion detection application (col.3 line 30 to line 37, and col.3 line 54 to col.4 line 1);

archiving event-data [raw, unprocessed alerts] associated with the frame [streams]; and
decoding [translation module 32] the event-data by a decode engine [aggregation, that is combining alerts produced by a single monitoring sensor] (col.6line 2 to line 5), the decode engine integrated within the intrusion detection application (col.4 line 1 to line 25).

Although the system disclosed by Porras shows all the features of the claimed limitation, but Porras does not specifically disclose *archiving* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

In an analogous art, Trcka, on the other hand discloses a network security and surveillance system passively monitoring surveillance traffic, such as network intrusion, by routing surveillance traffic [raw, unprocessed alerts] to Archival Media Unit (process 64, and item 80, Fig.3), such as database, and using archival data processing method for analysis (Fig.3, col.11 line 27 to line 48).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Porras and Trcka, because Trcka's method of archiving network traffic data would not only promote audit trail of a successful security attack in the system of Porras during monitoring of network intrusion but will also provide extent of damage caused by

Art Unit: 2131

intrusion traffic by performing playback (passive analysis) from traffic analysis of archived intrusion data, and thus not putting extra burden on latency of network traffic.

5. Claims 2, 5-6 are rejected applied as above in rejecting Claim 1. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 2, providing, by a network filter service provider (Porras: item 54, Fig.2) of the intrusion detection application, the event-data to an event-database (Porras: col.4 line 27 to line 40).

As to claim 5, generating a report from the decoded event-data; and providing the report to a report viewer (Porras: col.6 line 33 to line 52).

As to claim 6, providing, by the intrusion detection application, the decoded event-data to an intrusion detection client application (Porras: col.7 line 33 to line 55).

6. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras (U. S. Patent 6,704,874), as applied to claim 10, and further in view of Trcka et al (U. S. Patent 6,453,345).

Regarding Claim 11-13 Porras teaches a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method [Fig.6, col.9 line 1 to line 20] of:

- generating a report from the decoded intrusion related data (col.6 line 33 to line 52).

Although the system disclosed by Porras shows all the features of the claimed limitations, but Porras does not specifically disclose *archiving decoded (identified) data* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

In an analogous art, Trcka, on the other hand discloses a network security and surveillance system passively monitoring surveillance traffic, such as network intrusion, by routing surveillance traffic [raw, unprocessed alerts] to Archival Media Unit (process 64, and item 80, Fig.3), such as database, and using archival data processing method for analysis (Fig.3, col.11 line 27 to line 48).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Porras and Trcka, because Trcka's method of archiving network traffic data would not only promote audit trail of a successful security attack in the system of Porras during monitoring of network intrusion but will also provide extent of damage caused by intrusion traffic by performing playback (passive analysis) from traffic analysis of archived intrusion data, and thus not putting extra burden on latency of network traffic.

7. Claims 3, 7-9, and 14 are rejected applied as above in rejecting Claims 2, 6, and 11. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 3, providing the event-data to a decode server [remote processing center 26(server)] (Porras: col.4 line 33 to line 40).

As to claim 7, wherein the decoded event-data is formatted, by the client application, for display in a graphical user interface (Porras: col.7 line 19 to line 33).

As to claim 8, wherein the intrusion detection application runs locally on the first node [Fig.1 item 22 of network node 12] (col.3 line 19 to line 22).

As to claim 9, wherein the intrusion detection client application runs remotely on a second node, the first node and the second node operable to engage in a communication session between the client application and the intrusion detection application (Porras: col.3 line 30 to line 40, and col.7 line 19 to line 32).

As to claim 14, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of transmitting the decoded data to a client application (Porras: col.7 line 33 to line 55).

8. Claims 4, and 15 are rejected applied as above in rejecting Claims 3, and 14. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 4, wherein the decode server obtains the event-data from at least one of an event viewer and a report server [remote management interface 36] (Porras: col.3 line 23 to line 30, and col.6 line 28 to line 33).

As to claim 15, wherein transmitting the decoded data to a client application further comprises transmitting the report to a client application in communication with the intrusion detection application (Porras: col.3 line 30 to line 40, and col.7 line 19 to line 32).

Art Unit: 2131

9. Claim 16 is rejected applied as above in rejecting Claims 15. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 16, wherein transmitting the report to a client application further comprises transmitting the report to the client application in communication with the intrusion detection application (Porras: col.7 line 33 to line 55), the client application running remotely from the intrusion detection application (Fig.4, col.3 line 23 to line 26).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ

July 05, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100